

Re: Strange TCP behaviour

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.solaris/2004-05/2133.html>

From: Aashish Manocha (aashish.manocha_at_oracle.com)

Date: 05/28/04

Date: Fri, 28 May 2004 13:03:44 +0530

Hi,

"Bruno De Graef" <degraefb@hotmail.com> wrote in message
news:5da200e3.0405270108.3f55f1db@posting.google.com...

> *Hi all,*

>

> *I'll start be describing our current situation. We have an apache
> 1.3.19 (old version, I know it but we need it due to compatibility
> reasons with the application, an new version is in the pipe.) running
> as a reverse proxy. The host OS is running Solaris 2.8 with multiple
> virtual addresses defined for 1 interface. Clients (from remote sites
>) are connecting through VPN towards this reverse proxy.*

>

> *However since 2 weeks clients are complaining from timeouts from time
> to time in the browser, where they need to refresh there page. After
> having sniffed the network – client / server / switch – (because
> nothing was showing up in log files) we found the following strange
> behaviour in the TCP session.*

>

I tried to understand this behaviour, but am not sure if details
provided are correct. Based on following :

> 1. *Client SYN => Server*

> 2. *Server ACK => Client ????????*

> 3. *Client RST => Server*

> 4. *Client SYN => Server*

> 5. *Server SYN ACK => Client*

> 6. *Client ACK => Server*

> 7. *Server ACK => Client*

>

a] Client had send the SYN to Server (statement 1), Server replies
back with ACK only ??

– I believe this should have been SYN/ACK, and if not, then is it
a packet to some earlier connection.

b) Client sends reset to this ACK, why should it send a reset, may be because,
– it was expectnig a SYN/ACK
– or there is something wrong in the ACK packet, possibly the target port number, wrong ACK etc.

c) Statement 7, What did server ACK here.

I have assumed that the 7 statement, above are in sequence of what is happening,

> *As you can see the tree-way handshake is disturbed by the server sending and ACK to the client with a higher packet number on the initial SYN request.*

>
> *We are completely lost on the issue. Even our Telecom guys can't explain the behaviour. Therefore we would like some advise on how to explain the behaviour.*

>
> *Please find here a description on our architecture :*
> *< Server 1 > – <SWITCH> – <Loadbalancer > – <Firewall> – <VPN> – <NAT > Firewall> – <Switch> – <Client PC>*

–One more thing, Loadbalancer is here, is "web acceleration" configured on it,

what type of load balancing it is doing, is it layer 4 or layer 7. or simply giving away the connection request to the servers in round robin fashion.

If the packet captures from 3 locations can be provided, I think it would be very easy to find the culprit.

- 1] At server
- 2] At load balancer, Firewall end.
- 3] At Client.

It is highly probable that, there is something in Loadbalancer configuration.

Regards
–Aashish Manocha